ELSEVIER

Journal of Pure and Applied Algebra 153 (2000) 17–25

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Fast recognition of alternating and symmetric Galois groups

J.H. Davenport *, G.C. Smith

School of Mathematical Sciences, University of Bath, Bath BA2 7AY, UK

Received 28 November 1996; received in revised form 3 March 1999
Communicated by M.-F. Roy

Abstract

If a polynomial over $\mathbb{Q}$ is written down "at random", then its Galois group will, with probability 1, be S_n or A_n (see also Heintz (Theoret. Comput. Sci. 47(1986) 99–105)). However, if the polynomial arises through some mathematical operations, it is likely to have a much smaller Galois group. In this paper, we present probabilistic tests which will, for any polynomial, return either the answer "the Galois group is definitely one of S_n or A_n" or "the Galois group is likely to be smaller". The method involves reducing the polynomial modulo primes, using the Chebotarev Density Theorem and the properties of permutation groups.

MSC: 20P05; 12Y05

0. Introduction

It has been known for many years that the practical way to factor square-free rational polynomials is to factor them modulo p (primes dividing the leading coefficient need to be omitted) and then perform a Hensel lifting. In practice, it is normal to try several primes, and choose the best factorisation to lift. In fact the degrees of the irreducible factors mod p of a polynomial f (which we call the *shape* of f mod p) are the cycle lengths of an element of the Galois group of f over $\mathbb{Q}$. The Chebotarev density theorem [8] says that each possible shape occurs with the same frequency as the proportion of that cycle shape in the Galois group. Hence, if the Galois group is S_n, $1/n$ of whose elements are n-cycles, we will need approximately $n/2$ different primes before we have a 50% chance of choosing a prime such that the factorization modulo p is

* Corresponding author.
E-mail address: Davenport@bath.ac.uk (J.H. Davenport).

0022-4049/00/$ - see front matter
PII: S0022-4049(99)00078-X

irreducible, thus proving that the original polynomial is irreducible, i.e. that its Galois group is transitive.

Musser's calculations [10] suggest that, if we combine the data from different primes (e.g., when factoring a quartic, we can combine a 1.3 split modulo one prime with a 2.2 split modulo another to deduce that the polynomial is irreducible), rather than just waiting for irreducibility, then, transitivity can, with 50% probability according to experiments, be deduced in 5 probes (i.e. with 5 primes: note that a probe only returns a cycle shape, and not an actual permutation). Another way of saying this is that the median number of probes is between 4 and 5. In practice, one would want a higher degree of certainly — see the table at the end of this paper. Musser's experiments were carried out with "random" polynomials, and therefore apply when the Galois group is S_n or A_n (see also [6]). For other groups, the situation can be very different [3,9] have shown that, if the Galois group is S_n, then this can be recognised with probability $1-\varepsilon$ by a bounded number of probes, depending on ε but independent of n, and this result has been generalised to A_n [4].

We shall show that it is easy to verify that a Galois group is either A_n or S_n, and failure of verification in, say, four additional steps after showing transitivity, given that the Galois group is transitive on its roots, should be taken as strong evidence that the Galois group is not A_n or S_n. Here "strong" means that the probability of the test suggesting that the group is not S_n or A_n when in fact the group is one of these is $< 10\%$ (see [11, p. 24] for some experimental evidence).

We say that a finite permutation group is very transitive if it is at least 4-transitive. We first deal with showing that the group is (or providing evidence that it is not) very transitive, then we deal with the case of the very transitive groups that are not S_n or A_n.

1. Theory

The following result is a variation on a theorem of C. Jordan. Versions of the original formulation can be found both in [5] as Theorem 5.6.2, and in [12] as Theorem 13.2. These results all require the permutation group in question to be primitive. We wish to use the result when G is the Galois group of a polynomial, and in this circumstance is not necessarily an easy matter to detect primitivity. However, we are able to relax the primitivity to mere transitivity, and as we observed above, this is easy to detect. By way of compensation for weakening one condition, we have to strengthen the rest.

Theorem. *Let G be a transitive permutation group of degree n. Suppose that G has an element g of prime order p, where $n/2 < p < n-2$, then G is very transitive.*

Proof. Let $H = \langle g \rangle$ be the cyclic group generated by our element of order p. As a permutation it must be a p-cycle, since $p > n/2$. Thus H must act primitively on its support. Let $\mathscr{P}(m,t)$ be the set of subgroups S of G which act primitively and m-transitively on their supports of size t. Of course if $m > 1$, then the primitivity condition is redundant.

For v in the range $1 \leq v \leq n-p+1$ let $\mathcal{Q}(v)$ be the proposition that $\mathcal{P}(v, p+v-1) \neq \emptyset$. We shall prove by finite induction on v that $\mathcal{P}(n-p+1, n) \neq \emptyset$. Notice that $H \in \mathcal{P}(1, p)$ so $\mathcal{Q}(1)$ is true.

Suppose $\mathcal{Q}(v)$ is true for some $1 \leq v < n-p+1$, and we choose $K \in \mathcal{P}(v, p+v-1)$. Let $\Omega = \text{supp}(K)$ so $n/2 < p \leq |\Omega| < n$. The support of K is not a block of G since G is transitive of degree n but $|\Omega| \nmid n$. Thus there exists $l \in G$ such that $\Omega \neq \Omega l$ but $\Omega \cap \Omega l \neq \emptyset$. Choose such an l so that the order s of $C = \Omega \cap \Omega l$ is maximized.

Let A and B be the complements, both of size r, of C in Ω and Ωl, respectively. Conjugation by l induces an isomorphism of permutation groups between K and $l^{-1}Kl = K^l$. Thus $K^l \in \mathcal{P}(v, p+v-1)$ and it acts primitively on Ωl. Suppose, for contradiction, that $r > 1$. By primitivity of K^l there will exist $h \in K^l$ such that the number u of elements of B sent to elements of B satisfies $1 \leq u < r$, otherwise B would be a non-trivial block of K^l acting on Ωl. Thus exactly $r-u$ of the elements of B are transported to C by h, and of course there must be a balancing collection of $r-u$ elements of C transported from C to B by h. Consider K^h with support Ωh. The set Ωh consists of A unmoved by h together with the $r-u$ elements of B which, via h, are arrivals from C and a collection of $s+u-r$ elements of C. Thus $|\Omega \cap \Omega h| = r + (s+u-r) = s+u$ is greater than s but less than $s+r = |\Omega|$. This contradicts the maximality of s, so $r = 1$. Let $L = \langle K, K^l \rangle$ with support of size $p+v$. It is easy to see that L acts $(v+1)$-transitively and thus primitively on its support. We conclude that $\mathcal{Q}(v+1)$ is true.

By finite induction we obtain that $\mathcal{P}(n-p+1, n) \neq \emptyset$ so G contains a $n-p+1$-transitive subgroup of degree n, and G inherits this property itself.

What is the efficiency of this test? If $p > n/2$, then the fraction of elements of S_n with a p-cycle is $1/p$, so the chance of a single probe finding such an element is $\sum 1/p$ with $n/2 < p < n-2$, p prime. Heuristically, we can evaluate this (using the Prime Number Theorem) as

$$\sum_{\substack{n/2 < p < n-2 \\ p \text{ prime}}} \frac{1}{p} \approx \int_{n/2}^{n-2} \frac{1}{p \log p} \, \mathrm{d}p = [\log\log p]_{n/2}^{n-2} \approx [\log\log p]_{n/2}^{n}$$

$$= \log\log n - \log\log \frac{n}{2} = \log\left(\frac{\log n}{\log n - \log 2}\right)$$

$$= \log\left(1 + \frac{\log 2}{\log n - \log 2}\right) \approx \frac{\log 2}{\log n - \log 2}$$

(truncating the Taylor series at the first term). For $n = 20$, this would give 0.3010, as opposed to the true answer of $1/11 + 1/13 + 1/17 \approx 0.2267$ (the fact that 19 does not count is responsible for much of the error). This would give either 2 or 3 as the number of probes required to have a 50% chance of deducing that G is very transitive, assuming we already know that it is transitive. For $n = 200$, the formula gives 0.1505,

and the true answer is 0.1412. Both these values of n require 5 probes to have a 50% chance of deducing that G is very transitive. It is obvious from the formula that the number of additional probes is decreasing with n. The rate of decrease is not very fast, though, and we can easily approximate, or even compute, the number of probes required to give any degree of certainty (i.e. for all $\varepsilon > 0$, we can compute N such that N probes on S_n or A_n will detect that the group (known to be transitive) is very transitive with probability $> 1 - \varepsilon$: for $n = 100$ and $\varepsilon = 0.1$, N works out as 12.93, i.e. 13). □

2. Strengthening the theory

Note the rôle of the condition $n/2 < p$. It enters in two ways. First it ensures that the initial cyclic group of order p acts transitively on its support (if p were smaller then g might be, for instance, the product of two disjoint p-cycles). A single p-cycle acts primitively on its support because block sizes must be divisors of p. Of course, we can make this issue disappear for smaller p by insisting that g is a p-cycle.

Secondly we need to ensure that the groups we examine in the course of the proof have supports which are not blocks of G. Now, we can do this by assuming a priori (see [5] or [12]) that G is primitive, but we wish to avoid this, and we have seen how to do this when $p > n/2$. However, progress can sometimes be made even if $p < n/2$, subject to the hypothesis that G is transitive. Provided p does not divide n then we can begin as in the proof above, and the argument does not break down until we construct a group of degree $p+x$ dividing n. In this case there is the possibility that the support of the group we have built is a block of G and that what we have is an $x+1$-transitive group acting on this block.

For example, if you find a p-cycle in G where p is prime in the range $n/3 < p \leq n/2$ then either G is very transitive or has a block of size $n/2$. Note that these concerns are real. Let p be a prime and consider the wreath product of C_p by C_2. This group has natural representation of degree $2p$, acts transitively but imprimitively on these points, and contains an element which is a p-cycle.

Theorem. *Let G be a transitive permutation group of degree n. If r does not divide n or G contains an element x involving a cycle of length c coprime to $r!$ with $c > n/r$ then there cannot be blocks of size n/r.*

Proof. Since G is transitive, any block size must divide n, so r must divide n. Now, suppose a suitable c exists. If G had a block D of size n/r then D would have r translates under G. The group G would then act on this set of size r and for every $g \in G$ the element $g^{r!}$ will act trivially. Thus every $g^{r!}$ permutes the elements of D, and also permutes the elements of each translate of D. However, since the cycle involved in x has length coprime to $r!$ it follows that $x^{r!}$ involves a cycle of length $c > n/r = |D|$. This contradiction gets us home. □

For example suppose that $n = 100$ and that you know that G is transitive, and that G has a cycle of length 55 then there cannot be block of size 50. Now the existence of a 29-cycle is enough to force G to be very transitive.

3. On the absence of cycles of specified sizes

The distribution of cycle sizes of permutations is a much-studied subject, see [1]. We hope the following elementary result will be of interest.

Let $u \leq n$ be natural numbers. An element α of S_n is said to be r,u-homogeneous if it is the product of u pairwise disjoint r-cycles. A permutation is said to be *involved* in $g \in S_n$ exactly when g is the product of α and a permutation of disjoint support. Let $a_{n,u}$ be the cardinality of

$$\{(\alpha, g) | \alpha \text{ is } r,u\text{-homogeneous}, \alpha \text{ is involved in } g\}.$$

The quantity $a_{n,u}$ is easy to calculate. It is $n!/(r^u u!)$.

Let the number of elements of S_n involving exactly v r-cycles be $b_{n,v}$ and the number involving at least v r-cycles be $c_{n,v}$. Thus $c_{n,v} = \sum_{w=v}^{\infty} b_{n,w}$. The terms of this sum vanish when $wr > n$ of course.

Now $a_{n,j} = \sum_{i=j}^{\infty} \binom{i}{j} b_{n,i}$ so

$$a_{n,1} - a_{n,2} + a_{n,3} - \cdots = \binom{1}{1} b_{n,1} + [\binom{2}{1} - \binom{2}{2}] b_{n,2} + [\binom{3}{1} - \binom{3}{2} + \binom{3}{3}] b_{n,3} \ldots .$$

Thus by a standard binomial identity we have

$$c_{n,1} = \sum_{i=1}^{\infty} b_{n,i} = a_{n,1} - a_{n,2} + a_{n,3} - \cdots .$$

We conclude that the number of elements of S_n involving no r cycle is

$$n!(1 - (r^1 1!)^{-1} + (r^2 2!)^{-1} + \ldots + (-1)^l (r^l l!)^{-1}),$$

where rl is the largest multiple of r not greater than n. Fix r and select an element of S_n uniformly at random; the probability that this element involves no r cycle tends to $e^{-1/r}$ as $n \to \infty$. This generalizes the well-known result concerning car keys and hats when $r = 1$.

4. Very transitive groups

Thanks to the classification of finite simple groups, all very transitive permutation groups are known [2]. They must be symmetric or alternating, or one of four other permutation groups discovered by Mathieu. The four exceptional permutation groups have degrees $11, 12, 23$ and 24 are known as M_{11}, M_{12}, M_{23} and M_{24}. Both M_{11} and M_{23} are 4-transitive but not 5-transitive, whereas M_{12} and M_{24} are 5-transitive but not 6-transitive.

Now suppose that we are deploying our theorem on the Galois group G of a polynomial of degree n and we suppose that we have gathered enough data from probes so that we know G is transitive on the roots (i.e. the polynomial is irreducible in $\mathbb{Q}[\mathbb{X}]$). We seek to show that G is either A_n or S_n. If $n = 11$ (a prime) then p-cycles which reveal that G is very transitive have lengths 2, 3, 5 and 7. The worst prime is 7 and even that yields that G is $11 - 7 + 1 = 5$-transitive and so is not the merely 4-transitive M_{11}. In fact, S_{11} has a 68.44% chance of being shown to be either S_{11} or A_{11} in one probe (assuming that we already know that it is transitive), and A_{11} has a 61.33% such chance.

Similarly in degree 12, even if sticking to the $p > n/2$ regime and using the prime 7 we find that G is 6-transitive but M_{12} is only 5-transitive. However, the probability of success after n probes for S_{12} (assuming that we already know that the group is transitive) is $1 - (6/7)^n$, whereas using $p = 5$ as well (for which we have also to observe a 9-cycle or an 11-cycle), we get $1 - \left(\frac{454}{693}\right)^n - \left(\frac{247}{350}\right)^n + \left(\frac{17{,}453}{34{,}650}\right)^n$, whose 50% chance of success is after 3 probes rather than 5, and whose 90% chance of success is after 8 probes rather than 15. In degree 23 we can use all primes less than 23. The largest (and therefore the weakest) is 19 and even that yields that G is 5-transitive and so not M_{23}. In degree 24 we can use the primes 13, 17 and 19. Even the prime 19 yields that G is 6-transitive and so not M_{24}.

We need to know that there is a prime in the range $x/2 < p \leq x - 3$. We know that, for sufficiently large x, there is a prime in the range $x/2 < p < x/2 + (x/2)^c$ for any $c > \frac{7}{12}$ [7, formula 28.20], though "sufficiently large" is not made explicit. In practice, it seems that any $x \geq 8$ works.

Our method applies when $n \geq 8$. In the case $n = 7$ you need to pick up a 5-cycle in conjunction with Condition (a), (b) or (c) information. This then yields that G is 3-transitive. This is not normally good enough, since 3-transitive groups abound. Indeed, serendipity fails when $n = 7$ for the simple group of order 168 has a 3-transitive permutation representation of that degree. However A_7 or S_7 can be recognised to be very transitive from a probe which yields just a 3-cycle (probability 1/36 or 1/72), and S_7 can also be recognised to be very transitive from a probe which yields just a 2-cycle (probability 1/240). If, however, we add in that a 3.2^2 shape implies the existence of a simple 3-cycle, the probability for detecting that the group is very transitive given that it is transitive, when the group is in fact A_7, rises to $\frac{1}{9}$, and also when we consider that shapes 3.2 and 4.3 will imply a simple 3-cycle, and 5.2 will imply a 2-cycle, the probability for S_7 becomes $\frac{47}{144} \approx 0.33$.

Sometimes one can recognize that a group is 2-transitive from limited information gleaned from probes.

Proposition. *Let G be a permutation group of degree n. Suppose that one of the following conditions holds*:

(a) *G contains an n-cycle and an $(n-1)$-cycle* $(n > 2)$.

(b) *The degree n is odd and G contains an n-cycle and either an $n-2$-cycle or an $n-2$-cycle composed with the disjoint transposition* $(n > 3)$.

(c) *The degree n is even and G contains an $n-1$ cycle and an $(n-2)$-cycle composed with the disjoint transposition* $(n>2)$.

It follows that G is 2-transitive.

Proof. Condition (a) obviously forces G to be 2-transitive.

If condition (b) holds we may assume that G contains an $n-2$-cycle by squaring to remove the possible transposition. Let α be the given n-cycle and β the given $(n-2)$-cycle. Let a,b denote the fixed points of β. The order of α is odd so no power of α can transpose a and b. Conjugate β by the power of α which sends a to b to obtain $\gamma \in G$. Now γ is an $(n-2)$ cycle with fixed points b and c where $c \neq a$. Now conjugate β and γ by all possible powers of α to obtain a collection C of $(n-2)$-cycles. For each integer $i \in \{1,\ldots,n\}$ there are $c_i^1, c_i^2 \in C$ with i fixed by both c_i^1 and c_i^2 but the fixed point sets of c_i^1 and c_i^2 being distinct.

Suppose (r,s) and (u,v) are distinct ordered pairs of the elements being permuted. A suitable power of α will send r to u. Now either s and v are both in the support of c_u^1 or c_u^2 or s and v are fixed points of c_u^1 and c_u^2, we may assume respectively. In the first case we can use a power of the relevant c_u^m to take s to v. In the second case we first move s to the distinct point s' using c_u^2. Now both s' and v are not in the fixed point set of c_u^1 so a suitable power of c_u^1 will send s' to v and we are done.

Now we assume that condition (c) holds, and we allow ourselves to re-use notation. Let the given $(n-1)$ cycle be α and have fixed point a. Let β be the given $(n-2)$ cycle composed with the transposition (b,c). Suppose we have the special case $a=b$. Conjugating β by powers of α we obtain a collection of elements D consisting of $(n-2)$-cycles composed with all possible transpositions a,x as x varies over $G \setminus \{a\}$. Now conjugate α by each element of D in turn. We obtain elements of G consisting of $(n-1)$ cycles with every possible fixed point. These $(n-1)$-cycles are enough to render G 2-transitive.

Thus we may assume that we do not have the special case $a=b$. Conjugating α by a power of β we obtain an $(n-1)$-cycle α' with fixed points d different from a and b. Now conjugate β by a power of α sending b to d to obtain β' which transposes d and e. Now replacing α and β by α' and β' we are in the special case analyzed before and so we are done.

Now when G is known to be 2-transitive, and hence primitive, the fact that G is very transitive (and hence A_n or S_n) can be detected using any p-cycle in G where p is prime and less than $n-2$.

5. Computational experiments

The previous proposition is not necessarily very useful in practice. Condition (a) requires observing both an event with probability $(1/n)$ in S_n and an event with probability $1/(n-1)$, and therefore is rare (12 probes when $n=10$ for a 50% chance of success; 27 for a 90% chance). The statistics for the other conditions are similar.

Table 1
Number of probes for a given probability

n	Transitive			Very transitive		
	90%	95%	99%	90%	95%	99%
10	6	8	10	9	11	15
20	7	8	10	8	9	12
40	7	8	10	8	10	12
60	7	8	11	9	11	14
80	7	8	10	8	10	12
100	7	8	11	9	10	13
200	7	8	11	8	10	13

It is conventional to state, following Musser, that "5 probes are generally enough to prove transitivity". This statement has been analysed in [3], who shows that, not only is it certainly not true for groups such as V_4, which can never be proved transitive by studying factorizations modulo primes, but that, even for other groups, such as the Frobenius groups, it is far from being true. Is it true for S_n? The following table, extracted from [11], shows that to be reasonably certain (90% or more) that the group is transitive, by the Musser test, one needs more than 5 probes, and also that the additional cost (i.e. the difference between the columns) of testing for the group being very transitive by the algorithm of this paper is low (when the group is S_n).

It would appear from Table 1 that the number of probes is independent of n, as is the case in [9] (though they are dealing with actual permutations, rather than cycle shapes).

Conjecture. For a fixed probability ε, the number of tests required to ensure that the wrong answer, i.e. saying "probably not S_n or A_n" when in fact the group is one of these, is given with probability less that ε, is in fact bounded independent of n.

6. Conclusion

We wish to thank R.A. Parker who drew our attention to the possible relevance of a theorem in [5] to the question of Galois group recognition. We also thank Richard Puttock for his computational experiments [11], and the referee, whose comments improved the exposition.

References

[1] R. Arriata, A.D. Barbour, S. Tavaré, Poisson process approximations for the Ewens sampling formula, Ann. Appl. Probab. 2 (1992) 519–535.
[2] P.J. Cameron, Some multiply transitive permutation groups in: D. Jungnickel, S.A. Vanstone (Eds.), Coding Theory, Design Theory, Group Theory, Proceedings of the Marshall Hall Conference, Wiley New York, 1993, pp. 1–11.

[3] J.H. Davenport, Galois groups and the simplification of polynomials, Programmirovanie (1997) 43–58; English translation: Programming and Computer Science 23 (1997) 31–44.
[4] J.H. Davenport, Polynomial factorization, to appear.
[5] M. Hall, The Theory of Groups Macmillan, New York, 1959.
[6] J. Heintz, Polynomials with symmetric Galois group which are easy to compute, Theoret. Comput. Sci. 47 (1986) 99–105.
[7] M.N. Huxley, The Distribution of Prime Numbers: Large Sieves and Zero-Density Theorems, Oxford University Press, Oxford, 1972.
[8] J.C. Lagarias, A.M. Odlyzko, Effective versions of the Chebotarev density theorem in: A. Fröhlich (Ed.), Algebraic Number Fields, Academic Press, New York, 1977, pp. 409–464.
[9] T. Łuczak, L. Pyber, On random generation of the symmetric group, Combin. Probab. Comput. 2 (1993) 505–512, MR 95b:20004.
[10] D.R. Musser, On the efficiency of a polynomial irreducibility test, J. ACM 25 (1978) 271–282.
[11] R. Puttock, Computations in group theory, M.Sc. Thesis, University of Bath, 1996.
[12] H. Wielandt, Finite Permutation Groups, Academic Press, New York, 1964.